„Vertrauen gegen Vertrauen“
Die Zertifizierungsinstanz der Humboldt-Universität zu Berlin

Den immensen Nutzen privater und öffentlicher Netzwerke kann heute wohl niemand mehr bestreiten. Man kann über alle Grenzen hinweg Informationen austauschen, an gemeinsamen Dokumenten arbeiten und auf gleiche Datenbestände zugreifen. Der Tag, an dem Papier vollkommen aus Verwaltungsentscheidungen und Projektabläufen verbannt wird, liegt nicht mehr in allzu ferner Zukunft. Doch wie sieht es mit der Vertraulichkeit der transportierten Daten aus? Verdient Ihre elektronische Post nicht den gleichen Schutz, den Ihr geschriebener Brief hat? Die Gefahren oftmals herrschender Sorglosigkeit sollen hier als Denkanstoß kurz vorgestellt werden, und natürlich soll hier auch die Lösung präsentiert werden, die das Rechenzentrum der Humboldt-Universität zu Berlin für seine Benutzer geschaffen hat.

Welche Anforderungen muß man an eine Datenübertragung durch öffentliche und private Netzwerke stellen?

Vertraulichkeit	Nur der vom Absender bestimmte Empfänger muß in der Lage sein, die Nachricht zu lesen.
Authentizität	Der Empfänger muß in der Lage sein, zu überprüfen, ob die Information wirklich vom angegebenen Absender stammt.
Integrität	Die Information darf auf dem Weg vom Absender zum Empfänger nicht verändert werden.

Public Key-Verschlüsselung

Um essentiellen Anforderungen an eine sichere Kommunikation über unsichere Kanäle (das öffentliche Internet ist ein unsicherer Kanal) gerecht zu werden, muß man vertrauliche Daten unbedingt verschlüsseln. Wenn Verwaltungsentscheidungen rechtssicher durch elektronische Kommunikation unterstützt werden sollen, ist eine digitale Unterschrift zwingend erforderlich. Es gibt heute eine Vielzahl von Möglichkeiten, Daten suffizient zu verschlüsseln. Diese Verfahren müssen nicht unbedingt an eine Chipkarte gebunden sein, wie es einige Hersteller immer wieder suggerieren. Das Verschlüsseln bzw. Signieren von E-Mail ist u. a. mit dem Programm PGP („Pretty Good Privacy“) und dem Verfahren S/MIME („Secure Multipurpose Internet Mail Extension“) möglich. Beide Systeme arbeiten mit Public Key-Verschlüsselung. Dabei erzeugt jeder Benutzer ein asymmetrisches Schlüsselpaar, das aus einem privaten (Private Key) und einem öffentlichen Schlüssel (Public Key) besteht. Der private Schlüssel muß mit einer sogenannten Passphrase geschützt werden. Die Passphrase ist ein Paßwortsatz, der aus mindestens zwei Wörtern bestehen muß. Diese starke Passphrase soll davor schützen, daß der private Schlüssel gestohlen und von Unbefugten mißbraucht werden kann. Dies ist vor allem bei PCs oder anderen Systemen sinnvoll, die über keine geeignete Zugangskontrolle verfügen.

Um E-Mail nach dem Public Key-Verfahren zu verschlüsseln, muß der Absender den öffentlichen Schlüssel des Empfängers besitzen. Der darunterliegende Algorithmus stellt sicher, daß nur derjenige die E-Mail entschlüsseln kann, der im Besitz des dazugehörigen privaten Schlüssels ist. Ähnlich funktioniert eine digitale Signatur: der Empfänger kann die Gültigkeit der digitalen Signatur nur dann verifizieren, wenn er den öffentlichen Schlüssel des Unterzeichners hat.

Der Vorteil dieses asymmetrischen Verschlüsselungsverfahrens ist das Vorhandensein von mehr als einem Paßwort. Daher muß das Paßwort nicht vorher an den Kommunikationspartner übersendet werden. Der Nachteil liegt darin, daß man immer die aktuellen öffentlichen Schlüssel der Kommunikationspartner zur Verfügung haben muß. Die Kernfrage ist hier „Woher weiß ich, daß der Schlüssel authentisch ist?” Den öffentlichen Schlüssel seines Kommunikationspartners sollte man immer über einen anderen Weg erhalten als den, den man für die vertrauliche Kommunikation benutzen möchte, denn es ergibt keinen Sinn, sich den öffentlichen Schlüssel seines Kommunikationspartners per E-Mail schicken zu lassen, wenn man dann selbst diesen Kanal für die vertrauliche Kommunikation verwendet. Der Widerspruch dabei wäre nämlich: Ich traue diesem Kanal so wenig, daß ich darüber laufende E-Mail verschlüsseln will, akzeptiere aber einen öffentlichen Schlüssel, der mich über diesen unsicheren Kanal erreicht.

Möglich ist, sich den öffentlichen Schlüssel des Kommunikationspartners über das WWW oder einen der zahlreichen weltweit verbundenen PGP-Public-Key Server

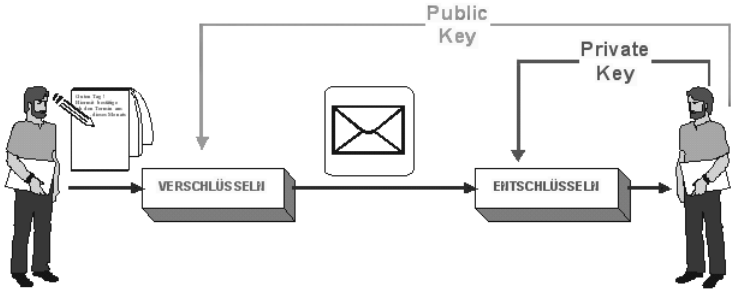

Abb. 1: Funktionsprinzip der Public Key-Verschlüsselung

(http://blackhole.pca.dfn.de/keyserver.html) zu besorgen, oder man vergleicht den Fingerprint (mathematisch erzeugter, einmalig auftretender Wert) des öffentlichen Schlüssels per Telefon.

Funktionsprinzip einer Zertifizierungsinstanz

Weniger umständlich und weniger vom Zufall abhängig ist der Einsatz einer Zertifizierungsinstanz. Die hauptsächliche Funktion einer Zertifizierungsinstanz

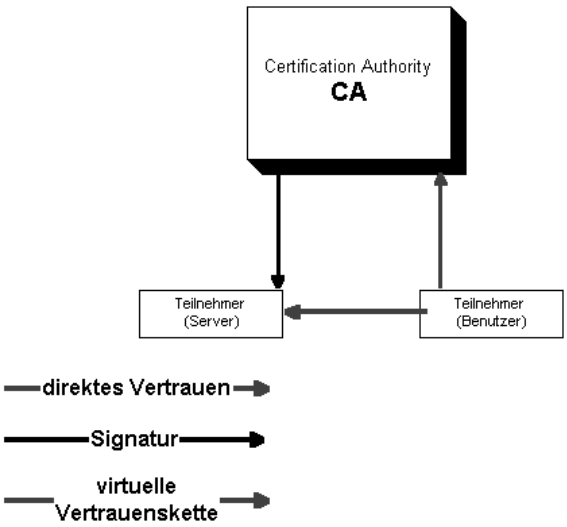

Abb. 2: Virtuelle Vertrauenskette innerhalb einer CA

(Certification Authority – CA) ist, zu bestätigen, daß ein ihr vorgelegter öffentlicher Schlüssel zu einer Person, Organisation oder Institution gehört. Sie bestätigt dies durch eine elektronische Signatur. Diese digitale Signatur wird an den jeweiligen öffentlichen Schlüssel angehängt. Der Empfänger einer E-Mail braucht nun nicht mehr jeden Absender einer signierten E-Mail zu kontakten, um die Echtheit des öffentlichen Schlüssels zu überprüfen. Es genügt, daß er den öffentlichen Schlüssel der Zertifizierungsinstanz besitzt, um deren Signaturen unter anderen öffentlichen Schlüsseln zu verifizieren. Dieses Vertrauen zu einer Zertifizierungsinstanz kann nur dann funktionieren, wenn sich die Zertifizierungsinstanz verpflichtet, nach einer bestimmten Richtlinie (Policy genannt) zu arbeiten. Die Genauigkeit und die Sorgfalt, mit der die Zertifizierungsinstanz arbeitet, ist die Basis für das Vertrauen, das der Benutzer zu dieser Zertifizierungsinstanz aufbaut. Dabei spiegelt solch eine Zertifizierungsinstanz eigentlich nur Vorgänge wider, die sich im täglichen Leben abspielen. Nehmen wir ein einfaches Beispiel: Ihnen wird von Ihrem Chef ein neuer Mitarbeiter vorgestellt. Sie zweifeln nicht an der Identität des neuen Mitarbeiters, da Sie wissen, daß Ihr Chef sich bei der Einstellung durch Überprüfung der Personaldokumente von der Identität des neuen Mitarbeiters überzeugt hat. Sie vertrauen Ihrem Chef, also vertrauen Sie allen, denen Ihr Chef vertraut. Es wurde eine „virtuelle" Vertrauenskette aufgebaut.

Wie sieht es nun konkret an der Humboldt-Universität zu Berlin aus? Mit Beschluß der Kommission für Rechentechnik des Akademischen Senats wurde am 16. Februar 1998 eine Zertifizierungsinstanz der Universität gegründet. Die Zertifizierungsinstanz nennt sich Humboldt-University Certification Authority, abgekürzt HU-CA.

Die Policy der HU-CA wurde von dieser Kommission bestätigt. Sie kann unter http://ca.hu-berlin.de/huca/huca-policy.phtml nachgelesen werden und ist für alle Teilnehmer bindend. Zwecks Erhaltung der Übersichtlichkeit ist die Gründung von Zertifizierungsunterinstanzen, sogenannter DCAs (Delegate Certification Authorities), vorgesehen. Diese DCAs unterschreiben ab sofort die öffentlichen Schlüssel der zur Teilnahme berechtigten Personen. Zum Zeitpunkt des Erscheinens dieses Artikels existiert innerhalb der HU-CA die DCA des Rechenzentrums (RZ-DCA), die im Rahmen der disponiblen Ressourcen alle Signaturen

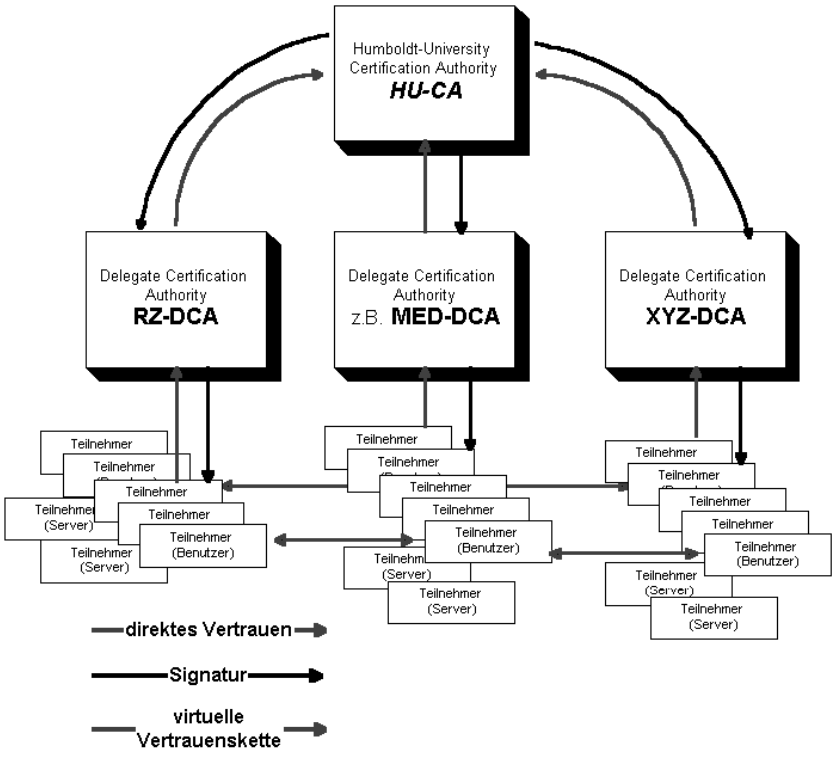

Abb. 3: Mögliche Vertrauensketten innerhalb der HU-CA

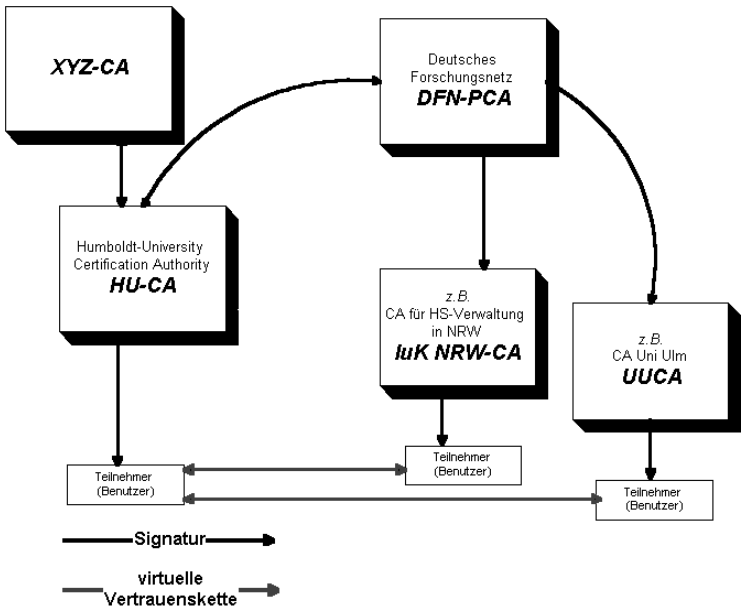

Abb. 4: mögliche Außenbeziehungen der HU-CA

vornehmen wird. Weitere Informationen finden Sie auf dem WWW-Server der HU-CA http://ca.hu-berlin.de/.

Indem die HU-CA Vertrauensbeziehungen mit anderen Zertifizierungsinstanzen eingeht, kann so ein weitreichendes Vertrauensnetz aufgebaut werden.

X509

Die HU-CA deckt nicht nur PGP-Signaturen ab. Ein wichtigerer Aufgabenbereich ist es, verschlüsselte Verbindungen im WWW zu ermöglichen. Durch das Ausstellen sogenannter Server-Zertifikate nach dem Standard X509v3 kann jeder Benutzer mit diesem Server eine verschlüsselte SSL-WWW-Verbindung aufbauen. Die Möglichkeiten, die eine solche Absicherung des WWW-Dienstes bietet, sind umfassend. Man kann so z. B. auch sensiblere Daten über diese verschlüsselten Kanäle anbieten. Dazu bedarf es keiner Änderung an Ihrem WWW-Browser. Die modernen Browser von Netscape und Microsoft sind in der Lage, SSL-Verbindungen zu einem entsprechenden WWW-Server aufzubauen. Sie müssen vorher nur das Wurzelzertifikat der ausstellenden Zertifizierungsinstanz in Ihren Browser einlesen. Nähere Informationen hierzu finden Sie unter http://ca.hu-berlin.de/hu-ca/help/. Jeder Administrator eines WWW-Servers sollte in Erwägung ziehen, einen sicheren SSL-WWW-Server zu installieren. Der Aufwand für die Installation und Konfiguration ist hierbei gering im Vergleich zum Nutzen, den man aus einem solchen Dienst ziehen kann. Sie sollten sich stets vergegenwärtigen, daß ein normaler Zugriff auf einen WWW-Server immer im Klartext geschieht und dieser Zugriff unterwegs abgehört oder verfälscht weitergeleitet werden kann. Es sind derzeit zahlreiche Softwareprodukte für die meisten Betriebssysteme im Freeware- und auch im kommerziellen Softwarebereich verfügbar (Apache-SSL, Stronghold, IIS, Netscape Suite Spot etc.). Nähere Hinweise zum Bestellen eines Server-Zertifikates für verschiedene WWW-Server bei der HU-CA finden Sie unter http://ca.hu-berlin.de/hu-ca/help/.

Um auch für den Serveradministrator die Vergabe der Zugriffsrechte zu vereinfachen, stellt die HU-CA auch sogenannte User Certificates (persönliche Zertifikate) aus. Diese persönlichen Zertifikate werden fest in Ihrem WWW-Browser gespeichert. Ein Paßwort schützt den unberechtigten Gebrauch dieses Zertifikates. Mit dem Zertifikat (das im Grunde genommen auch ein asymmetrisches Schlüsselpaar ist) können Sie sich gegenüber dem SSL-WWW-Server eindeutig identifizieren. Dieser SSL-WWW-Server kann sofort ein Vertrauensverhältnis zu Ihnen aufbauen, da er an Ihrem persönlichen Zertifikat die Signatur der HU-CA „erkennen“ kann. Da der Server allen Zertifikaten der HU-CA traut, traut er auch Ihnen über die oben besprochene „virtuelle“ Vertrauenskette.

Wenn Sie den Netscape Communicator oder den Microsoft Internet Explorer benutzen, können Sie mit diesem persönlichen Zertifikat auch E-Mail verschlüsseln oder digital signieren. Dies beruht auf dem von der amerikanischen Firma RSA Inc. entwickelten Standard S/MIME. Sie haben ein eigenes paßwortgeschütztes, asymmetrisches Schlüsselpaar (hier persönliches Zertifikat genannt) und verschlüsseln die E-Mail mit dem öffentlichen Schlüssel Ihres Empfängers. Bedingung hierfür ist, daß Sie ein persönliches Zertifikat besitzen. Dieses persönliche Zertifikat können Sie über den WWW-Server der HU-CA bestellen.

Namensgebung bei X509

Wie Sie der Policy der HU-CA entnehmen können, müssen die ausgestellten Zertifikate bestimmten Namenskonventionen folgen. X509 lehnt sich dabei an eine standardisierte hierarchisch aufgebaute Baumstruktur an. Die Identifikationen eines jeden Servers oder Benutzers innerhalb dieses Baumes nennt man Distinguished Name (DN). Der DN für einen Benutzer des Rechenzentrums könnte z. B. wie in Abb.5 lauten. Durch diese streng hierarchische Struktur ist es sehr einfach, Abteilungen und Institute zu beschreiben und in eine globale Struktur einzuordnen. Dieses System erleichtert es auch, einem SSL-WWW-Server Admini-

```
cn=Alexander Geschonneck, ou=Rechenzentrum, o=Humboldt-Universitaet zu Berlin, c=DE
```

Abb. 5: Beispiel für einen DN

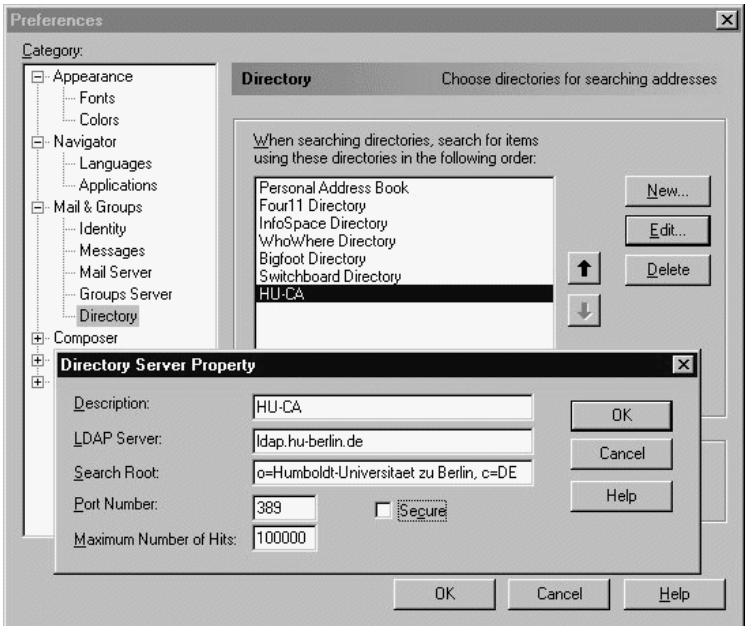

Abb. 6: Konfiguration des Zugriffs auf den Verzeichnisdienst der HU-CA mit dem Netscape Communicator

stratorzugriffsrechte nur für die Universität oder eine andere Einrichtung zu vergeben. Die verwendeten Algorithmen und die Arbeitsweise bzw. Policy der HU-CA stellen sicher, daß sich kein falscher Benutzer hinter einem Zertifikat verbirgt. Nähere Informationen finden Sie auf dem WWW-Server der HU-CA (http://ca.hu-berlin.de/).

Die ausgestellten Zertifikate werden in einem Verzeichnisdienst den Benutzern zu Verfügung gestellt. Dieser Verzeichnisdienst ist ein X500-Directory, auf das man mit einem LDAP-fähigen Tool zugreifen kann.

Unabhängig davon kann man über die Homepage der HU-CA mit jedem WWW-Browser den X500-Teilbaum erkunden. Es sind aber nur diejenigen Benutzer und Server enthalten, die von der HU-CA zertifiziert wurden und einer Veröffentlichung ihres Zertifikates ausdrücklich beim Antrag zugestimmt haben. Die Teilbäume Deutschlands und des DFN finden Sie unter http://x500.tu-chemnitz.de/ bzw. http://ambix.uni-tuebingen.de/. Der Verzeichnisdienst der HU-CA bietet erstmalig jedem Benutzer die Möglichkeit, ein Zertifikat durch Vergleich des Fingerprints auf dessen Gültigkeit zu überprüfen.

PGP

PGP ist eines der populärsten Verschlüsselungsprogramme, nicht nur im Internet. Die Versionen bis 2.6.3 sind Freeware. Es gibt viele Shareware- oder Freeware-Tools, mit denen man seine gewohnte Mailoberfläche „PGP-fähig" machen kann. Seit der Version 5 wird PGP auch als kommerzielles Produkt vertrieben. Es gibt aber weiterhin eine Freeware-Version, bei der einige Funktionen eingeschränkt sind. So kann die Freeware-Version keine RSA-Schlüssel erstellen. Dies bedeutet, daß die weitverbreitete Version 2.6.x Signaturen, die mit den neuen Schlüsselformaten erstellt wurden, nicht mehr überprüfen kann. Wer also zur Mehrheit der Internetgemeinde kompatibel bleiben möchte, muß sich entweder die kommerzielle Version PGP 5.5 kaufen oder einen mit PGP 2.6.x erstellten RSA-Schlüssel in die Version 5 importieren.
Wenn Sie mit PGP 2.6.x ein Schlüsselpaar erzeugen, müssen Sie folgende Befehlszeile eingeben:

```
c:\pgp\pgp -kg 2048
```

Bei der Erstellung neuer Schlüssel ist eine Schlüssellänge von 2048 Bit empfehlenswert. Die Key-ID muß unbedingt Ihren Namen und eine gültige E-Mail-Adresse der Humboldt-Universität zu Berlin beinhalten:

```
Alexander Geschonneck <geschonneck@rz.hu-berlin.de>
```

Den so erstellten Schlüssel extrahieren Sie mit `c:\pgp\pgp -kxa Dateiname` in eine Datei, die Sie dann zur Unterschrift einreichen.

Wenn die HU-CA Ihren Schlüssel unterschrieben hat, können Sie die neue Signatur mit `c:\pgp\pgp -ka Dateinname_mit_Signatur` wieder einlesen.

Leider verfügen die aktuellen 5er Versionen von PGP über ein paar grundlegende Mängel, so daß von der HU-CA derzeit nur RSA- und keine(!) DSS/DH-Schlüssel signiert werden. Weitere Hinweise finden Sie unter http://ca.hu-berlin.de/help/.

Die 5er Versionen beinhalten eine leicht zu erlernende Oberfläche und Plug-Ins für die Mailprogramme Eudora und Exchange. Weiterhin bietet PGP 5 die Möglichkeit, auf einen PGP-Keyserver zuzugreifen. Die HU-CA betreibt auch einen solchen Server. Sie müssen Ihr Programm auf die Adresse ca.hu-berlin.de

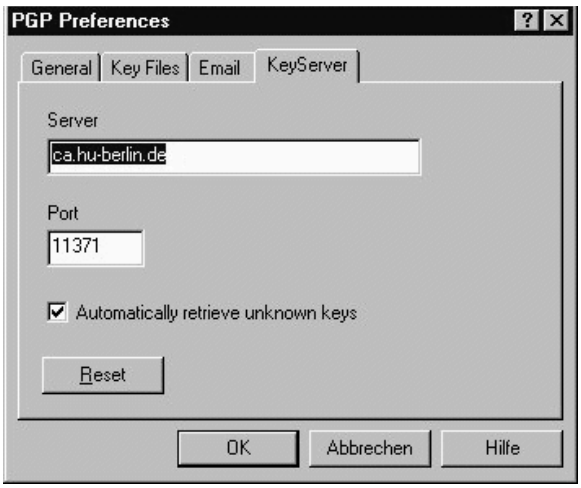

Abb. 7: Konfiguration des PGP-Keyservers der HU-CA mit PGP5

Port 11371 konfigurieren. Unabhängig davon kann man über die Homepage der HU-CA mit jedem WWW-Browser nach PGP-Schlüsseln auf dem PGP-Keyserver suchen.

Gültige Schlüssel

Abschließend veröffentlichen wir noch die Parameter der Schlüssel der HU-CA und RZ-DCA, damit Sie die Angaben im Internet überprüfen können.
Hinweise zur verwendeten Software und deren Bezugsquellen finden Sie auf der Homepage der HU-CA.

HU-CA

	Seriennr./KeyID	*Größe*	*Erstellt am*	*Gültig bis*	*Fingerprint (MD5)*
PGP	0x72A77495	2048Bit	27.11.97	27.11.00	57 0F 88 7B 7C 91 50 A8 2F B9 3E CA C2 06 31 E6
X509	01	1024Bit	30.03.98	29.03.00	D4:3B:59:3E:D6:E6:A9:BC:71:F6:A2:77:97:55:09:18

RZ-DCA

	Seriennr./KeyID	*Größe*	*Erstellt am*	*Gültig bis*	*Fingerprint (MD5)*
PGP	0x9FE88879	2048Bit	27.11.97	27.11.00	1D 05 B4 17 77 2E BF A9 98 64 80 A5 62 5E B3 20
X509	02	1024Bit	30.03.98	29.03.00	B8:D1:B9:21:85:63:2A:63:D6:83:64:7E:D0:19:AC:F2

Kontaktinformation

Humboldt-Universität zu Berlin
Rechenzentrum
HU-CA
Unter den Linden 6
D-10099 Berlin

Tel: 2093-2482
Fax: 2093-2959
WWW: http://ca.hu-berlin.de/
E-Mail: hu-ca@hu-berlin.de

Alexander Geschonneck
geschonneck@rz.hu-berlin.de
http://www.hu-berlin.de/~h0271cbj/